BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 33-152

1 JUNE 2012

Communications and Information

USER RESPONSIBILITIES AND GUIDANCE FOR INFORMATION SYSTEMS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-publishing.af.mil/.**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A3CP/A6CP

Certified by: AF/A3C/A6C
(Maj Gen Earl Matthews)

Supersedes: AFI33-100, 19 November 2008;
AFI33-113, 6 February 2007;
AFI33-119, 24 January 2005;
AFI33-127, 1 May 1998; and
AFMAN33-128, 1 March 1997

Pages: 36

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Information Resources Management*, AFPD 33-2, *Information Assurance (IA) Program*, and identifies policies and procedures for the use of cyberspace support systems/services and compliance requirements of Secretary of the Air Force, Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6) managed programs. These programs ensure availability, interoperability, and maintainability of cyberspace support systems/services in support of Air Force mission readiness and warfighting capabilities. This manual applies to all Air Force military, civilians, contractor personnel under contract by the Department of Defense (DOD), and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. This manual applies to the Air National Guard (ANG) and the Air Force Reserve Command (AFRC). **Failure to observe the prohibitions and mandatory provisions of this instruction as stated in paragraphs 3.2, 4.5.4.2, 4.10.1, and 5.1.1.2 by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ)*, Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to local laws and the terms of the contract. Additionally violations of paragraph 3.2 by ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.** Direct questions or comments on the

contents of this instruction, through appropriate command channels, to Cyberspace Operations, Cyberspace Policy Division (AF/A3CP/A6CP). Send recommended changes and conflicts between this and other publications, using Air Force (AF) Form 847, *Recommendation for Change of Publication*, to AF/A3CP/A6CP, with information copy to SAF/CIO A6, Policy and Compliance Division (SAF/A6PP). This publication may be supplemented at any level, but all direct supplements must be routed to the OPR of this publication for coordination prior to certification and approval. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force *Records Disposition Schedule (RDS)* located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See Attachment 1 for a glossary of references and supporting information.

SUMMARY OF CHANGES

This is a total revision to replace and update AFI 33-100, *User Responsibilities and Guidance for Information Systems*. It incorporates and replaces AFI 33-113, AFI 33-119, AFI 33-127, and AFMAN 33-128. It incorporates guidance for responsible use of the Internet that was previously covered by AFI 33-129, *Web Management and Internet*. This manual was rewritten and must be completely reviewed.

Chapter 1

INTRODUCTION

1.1. Introduction. In an effort to meet the growing needs of today's war fighter, great strides are being made to improve the capabilities offered by the Air Force provisioned portion of the Global Information Grid (GIG). Today's Air Force is increasingly using these capabilities in almost all activities of warfighting and operations support. This increased reliance on technology and its integration requires each individual to take responsibility for ensuring effective, efficient, and authorized use of these resources as they carry out their responsibilities.

1.2. Applicability. This publication applies to all Air Force Information Systems (ISs) and devices, including stand-alone ISs, IS components of weapon systems where Platform Information Technology (PIT) interconnections exist, ISs connected to external networks via authorized Internet Service Providers, ISs that provide the management infrastructure, and connections among other ISs and ISs used to process, store, display, transmit, or protect Air Force information, regardless of classification or sensitivity.

1.2.1. This publication is binding on all authorized users to include military, civilian, contractor, temporary employees, volunteers, and interns who are authorized to operate the ISs owned, maintained, and controlled by the Air Force.

1.2.2. More restrictive Federal, DOD, and Office of the Director of National Intelligence directive requirements governing non-Air Force space, Special Access Programs (SAP)/Special Access Requirements (SAR), and Intelligence information take precedence over this publication.

1.3. Objective. The objective of this publication is to ensure users understand how to protect and secure United States (US) government information processed by Air Force ISs with the assistance of their applicable organizational IA workforce personnel (e.g., organizational Information Assurance Officers [IAOs], Client System Technicians [CSTs]). This publication identifies policies and procedures for the use of cyberspace support systems/services and compliance requirements of Secretary of the Air Force, Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6) managed programs.

1.4. Assistance. Users contact the organizational IAO for clarification on any Information System requirements outlined within this publication.

1.5. Waiver Authority. AF/A3CP/A6CP is the waiver authority for the provisions in this manual. Waiver requests shall contain compelling justification and must be submitted via emailto AF/A3CP/A6CP.

Chapter 2

INFORMATION SYSTEMS AND END USER DEVICES

2.1. Overview. Information systems are a set of information resources. End user devices include ISs such as desktop PCs, laptops, notebooks, tablets, smartphones, executive mobile devices, etc. as used by users. Access control is one of the measures taken to ensure ISs are protected against threats and vulnerabilities. This chapter provides user responsibilities for ISs including end user devices whereas AFMAN 33-282, *Computer Security* provides policies for all Air Force ISs including IAO responsibilities for ISs.

2.2. Training Requirement. All IS users will complete DOD IA training prior to granting access to an IS according to DOD 8570.01-M, *IA Workforce Improvement Program*.

2.2.1. Users reaccomplish IA training annually using the Advanced Distributed Learning System (ADLS) computer based training which reports compliance to the IAO.

2.2.2. When a user requires a new account or modification to an existing account (due to change of station or assignment, Temporary Duty [TDY], etc.), users are not required to retake the DOD IA training provided the user has a valid and current (within a year) course completion record.

2.3. Information System Access. Access to an Air Force IS is a privilege and continued access is contingent on personal conduct, personnel actions, changes in need to know, or operational necessity. Users request IS access and specific authorizations within the system through the organization or system IAO using the DD Form 2875, *System Authorization Access Request (SAAR)*. DD Form 2875 signatures may be handwritten or digital. Contact the organization or system IAO for identification and authentication guidance and see AFMAN 33-282, *Computer Security*. See paragraph 2.14 for wireless mobile device requirements.

2.3.1. All authorized IS users will sign the standardized AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision* prior to initial IS access and submit to the organization IAO with a handwritten or digital signature. Only one AF Form 4394 is required per user as maintained by the organization IAO regardless of the number of system access requests inside or outside the organization.

2.3.2. Access to classified ISs also requires a Standard Form 312, *Nondisclosure Agreement*, according to AFI 31-401, *Information Security Program Management*.

2.3.3. Users may transport or email their user agreement (AF 4394) upon permanent change of station and present it to the gaining organization IAO at in-processing. Wireless Mobile Device user agreements must be reaccomplished due to new authorizing/issuing personnel.

2.3.4. Each user is responsible and accountable for their password/Personal Identification Number (PIN).

2.3.5. Users must protect all passwords and PINs based on the sensitivity of the information or critical operations they protect (e.g., a password used to gain access to a SECRET network is itself classified SECRET). Follow all CAC individual responsibilities according to AFI 36-3026_IP, Volume 1, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*.

2.3.6. Interim system access may be granted for less than 5 duty days if system access is required to complete electronic versions of DD Form 2875 and/or AF Form 4394.

2.3.7. DoD Visitor access allows any user with a DoD Common Access Card (CAC) temporary access on any supported computer when they are away from their normal duty station. This allows for limited access to the basic capabilities of the computer to enable access to available enterprise capabilities. Full access and privileges to additional capabilities requires a request for IS access.

2.4. Loss of Access. User's conduct that is inconsistent with IA policies and guidelines may result in immediate suspension of access to unclassified and classified ISs.

2.4.1. Supervisors follow the guidance in AFMAN 33-282, *Computer Security* for suspension actions once a violation is confirmed. Violations of IA policies and guidelines include, but are not limited to:

2.4.1.1. Unauthorized use of the network.

2.4.1.2. Failure to maintain annual DOD IA awareness training.

2.4.1.3. Actions that threaten the security of a network or a governmental communications system (e.g., willful downloading of malicious software, attempting to add unauthorized software, unauthorized flash drive usage).

2.4.1.4. Actions that knowingly threaten or damage DOD IS or communications security (hacking or inserting malicious code or viruses, theft, destruction of IT assets, willfully not using encryption).

2.4.2. If an individual's security clearance is suspended or revoked, access to IS will be suspended. If an organizational commander feels the member should have access restored on an interim basis, they shall follow reinstatement procedures outlined in AFMAN 33-282.

2.5. Disabling Accounts. Supervisors and/or users are responsible for notifying system privileged users (e.g., CSTs) or the IAO when an account is no longer required (e.g., individual leaves organization for local accounts or service for enterprise accounts) or if it is believed the account has been compromised.

2.6. General Protection. All authorized users will protect networked and/or stand-alone ISs against tampering, theft, and loss. Protect ISs from insider and outsider threats by controlling physical access to the facilities and data by implementing procedures identified in Joint, DOD, AF publications, and organizationally created procedures.

2.6.1. Backing up personal data stored locally on an IS (e.g. desktop computer, laptop) is the responsibility of the user. Local organizational policy dictates frequency and limitation factors.

2.6.2. Protect sensitive information (e.g. Controlled Unclassified Information [CUI], For Official Use Only [FOUO], Personal Identifiable Information [PII], Health Insurance Portability and Accountability Act [HIPAA], Privacy Act [PA], proprietary, contracts, etc.) with encryption when transmitting data.

2.7. Notice and Consent to Monitoring. Users of DOD telecommunications devices and information systems are to be notified the use of these systems constitutes consent to monitoring.

2.7.1. All users of DOD information systems will sign the standardized AF Form 4394. Local organizational commanders must restrict access to DOD information systems for those personnel who fail to sign the agreement. Organization IAOs are required to report to the Enterprise Service Desk (ESD) any failures to sign the agreement for revocation of access to enterprise capabilities.

2.7.2. To maintain continuous notifications to all users using DOD telecommunications devices including Voice over Internet Protocol (VoIP) phone instruments, user will report to the IAO any of following deficiencies:

2.7.2.1. A DD Form 2056, *Telephone Monitoring Notification Decal***,** is missing or not readable on the front of all official telephones and VoIP phone instruments.

2.7.2.2. A DD Form 2056 is missing or not readable on fax machines.

2.7.2.3. Locally created organizational/unit fax cover sheets do not contain the exact notice and consent statement: "Do not transmit classified information over unsecured telecommunications systems. Official DOD telecommunications systems are subject to monitoring. Using DOD telecommunications systems constitutes consent to monitoring."

2.7.3. The banner on DOD information systems functions to remind users of the conditions that are set forth in the AF Form 4394, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references the AF Form 4394.

2.8. Information Technology Asset Procurement. Procurement activities must adhere to AFI 33-112, *Information Technology Hardware Asset Management*.

2.8.1. Adhere to locally defined requirements process when acquiring IT hardware, cellular, and peripheral devices (e.g., desktops, laptops, servers, smartphones, cell phones, printers, scanners).

2.8.2. The installation Communications and Information Systems Officer (CSO) supports the information systems requirements process enabling requesting organizations to obtain new communications and information capabilities. Contact the AFWay, NETCENTS, or NETCENT-2 program management offices for purchase of information technology products and services using an enterprise procurement contract before locally acquiring information technology.

2.9. Communications and IS Relocations or Modifications. Contact the IAO prior to any project to install, relocate, modify, or remove end user devices. The IAO will provide guidance before initiating any project to install, relocate, modify, or remove end user devices to ensure the user submits requests in accordance with organizational policy.

2.10. Hardware and Software Security. Coordinate with the Information System Owner (ISO) and/or system Information Assurance Manager (IAM), and contracting office for security approval required as a part of any software purchase. Do not install software or hardware on an IS without coordination with the system IAO. The system IAO is responsible for the proper coordination and implementation in accordance with AFI 33-200, *Information Assurance (IA) Management* and AFMAN 33-282, *Computer Security*.

2.11. Malicious Logic Protection. Protect ISs from malicious logic (e.g., virus, worm, Trojan horse) attacks by applying a mix of human and technological preventative measures. Contact the IAO for additional guidance to protect ISs from malicious logic.

2.11.1. Scan approved removable media devices for viruses before and after use if scans are not automated.

2.11.2. Report any suspected IS abnormalities (i.e., antivirus errors, virus alerts, unexpected file size increases, unexpected disk access, strange activity by applications, etc.) immediately to the organizational IAO.

2.12. Privately-Owned Hardware and Software. Using privately-owned hardware and software for government work is strongly discouraged; however, it may be used for processing unclassified and sensitive information with justification and approval. Contact your organizational IAO for assistance and requirements and see AFMAN 33-282, *Computer Security*.

2.12.1. Do not connect or use any privately-owned media or peripheral devices (including but not limited to music/video CD/DVDs, digital music players, mobile phones, tablets, Universal Serial Bus [USB] drives, external hard drives, and flash media devices) to AF ISs and government furnished equipment (GFE).

2.12.2. Do not install and use copies of government-owned software on a home computer unless the software license explicitly allows users to do so and the installation CSO has authorized such use. Reference AFI 51-303, *Intellectual Property--Patents, Patent Related Matters, Trademarks and Copyrights*.

2.13. Peripheral Devices. A computer peripheral is any external device that provides input and output for the computer (e.g. mouse, scanners, smart boards, pointers, and keyboard devices are input devices). Do not connect any peripheral device not already preapproved for use on the AF-GIG without notifying the IAO.

2.14. Mobile Computing Devices. Mobile computing devices are IS devices such as Portable Electronic Devices (PED), laptops, and other handheld devices that can store data locally and access AF-managed networks through mobile access capabilities.

2.14.1. All authorized wireless mobile device users will sign the standardized AF Form 4433, *US Air Force Unclassified Wireless Mobile Device User Agreement*, and adhere to guidance contained within the agreement when using a wireless mobile computing device. The AF Form 4433 is not required for mobile computing devices issued with wireless capabilities disabled.

2.14.2. Encrypt all sensitive information (e.g. Controlled Unclassified Information [CUI], For Official Use Only [FOUO], Personal Identifiable Information [PII], Health Insurance Portability and Accountability Act [HIPAA], Privacy Act [PA], proprietary, contracts, etc.) transmitted through a commercial or wireless network (e.g., mobile hotspot, commercial Internet café) using an encrypted Virtual Private Network (VPN) connection or other authorized encryption solution whenever practical. Contact the Enterprise Service Desk (ESD) or see your base Communications Focal Point (CFP) for installation and usage instructions.

2.14.3. Do not operate unclassified wireless technology, devices or services (used for storing, processing, and/or transmitting information), in areas where classified information is discussed, electronically stored, electronically processed, or electronically transmitted without approval of the organizational IAO. See AFMAN 33-282, *Computer Security* for additional guidance.

2.14.4. Only use approved classified wireless devices to store, process, or transmit classified information.

2.14.5. Lost or stolen government mobile computing devices must be reported immediately to your IAO.

2.14.6. Complete additional PED and removable storage media training at the organization's discretion here: **http://iase.disa.mil/eta/pedrm_v2/pedrm_v2/launchPage.htm**.

2.14.7. Do not alter or remove any pre-installed software/configurations on end user devices without contacting the IAO.

2.15. Removable Media. Removable media refers to information system storage media that can be removed from its reader device, conferring portability on the data it carries (e.g., diskettes, CDs, DVDs, USB storage devices, or any other device on which data is stored and which normally is removable from the system by the user or operator).

2.15.1. Safeguard, mark, and label removable media according to the requirements for the highest level of information contained on the media using applicable information security guidance in AFI 31-401, *Information Security Program Management* and AFI 33-332, *Air Force Privacy Program*. External and internal labeling guidance for media can be found in AFMAN 33-363, *Management of Records*.

2.15.2. Do not remove removable media with sensitive information from protected workplaces unless encrypted with an authorized encryption method and signed in and out with a supervising official. Contact the IAO for specific guidance.

2.15.3. Immediately report loss or suspected loss of removable media containing classified, CUI, or PII to the IAO and according to AFI 31-401, *Information Security Program Management* and AFI 33-332, *Air Force Privacy Program*.

2.15.4. Obtain guidance and/or approval from the organizational IAO before attaching any external storage devices (to include USB storage devices, hard drives, and flash media) to an IS.

2.15.5. Immediately contact the IAO if it appears information of higher classification introduced onto a lower classification IS or there is spillage between compartments. Disconnect the suspected systems from the network and/or power off and secure the device appropriately.

2.15.6. Writing to any type of removable media from classified systems is prohibited unless appropriately approved. Organizations with a mission requirement to write to removable media must first submit requests for a waiver through the IAO.

2.16. Collaborative Computing. Collaborative computing (video teleconferencing, etc) provides an opportunity for a group of individuals and/or organizations to share and relay information in such a way that cultivates team review and interaction in the accomplishment of

duties and attainment of mission accomplishment. Contact the IAO for guidance on connecting video cameras and microphones to ISs.

2.17. Public Computing Facilities. Do not use public computing ISs (Internet cafés and kiosks, hotel business centers, etc.) for processing government-owned unclassified, sensitive or classified information. Public computing ISs include any information technology resources not under your private or the United States (US) Government's control.

2.17.1. Using these resources to access web-based government services (e.g., webmail) constitutes a compromise of log-in credentials and must be reported to your IAO.

2.17.2. Connection of privately owned or United States (US) Government controlled mobile computing devices to public networks is permitted to remotely access government services (e.g., webmail) if mobile computing device encryption and connection policies are followed. Public networks include internet service providers for private residences.

2.18. Security Incident Reporting. A security incident is an assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an IS. Security incidents can include but are not limited to:

2.18.1. Data Spillage. Data spillage occurs when a higher classification level of data is placed on a lower classification level system/device or across compartments.

2.18.2. Classified Message Incidents. A classified message incident occurs when a higher classification level of data is transferred to a lower classification level system/device via messaging systems. Users must:

2.18.2.1. Report all suspected and/or actual unauthorized network activities or incidents to the IAO ensuring notification continues up the chain of command. Use appropriate systems and methods to report incidents including secure voice if required or appropriate. Do not allow the incident to become widespread knowledge. Exercise "Need to know" in these situations.

2.18.2.2. Security incident response must include appropriate tasks to secure the computing environment from further malicious activity and preserve computer forensic evidence for analysis. User must disconnect affected IS or media from the network (i.e. removal of network cable, turn off wireless capability, etc.). Do not turn off the IS.

2.18.2.3. User notifies IAO or other designated representative as outlined in local operating instructions such as the Unit Security Manager (USM). USM notifies the wing Information Protection (IP) office within 24 hours of incident.

Chapter 3

RESPONSIBLE AND EFFECTIVE USE OF INTERNET-BASED CAPABILITIES

3.1. Limited Authorized Personal Use. Government-provided hardware and software are for official use and limited authorized personal use only. Limited personal use must be of reasonable duration and frequency that have been approved by the supervisors and do not adversely affect performance of official duties, overburden systems or reflect adversely on the Air Force or the DOD.

3.1.1. All personal use must be consistent with the requirements of DOD 5500.7-R, *Joint Ethics Regulation.*

3.1.2. Internet-based capabilities are all publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. Internet-based capabilities include collaborative tools such as SNS, social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps).

3.1.2.1. When accessing Internet-based capabilities using Federal Government resources in an authorized personal or unofficial capacity, individuals shall comply with OPSEC guidance (AFI 10-701, *Operations Security*) and shall not represent the policies or official position of the Air Force or DOD.

3.1.3. Examples of authorized limited personal use include, but are not limited to:

3.1.3.1. Notifying family members of official transportation or schedule changes.

3.1.3.2. Using government systems to exchange important and time-sensitive information with a spouse or other family members (i.e., scheduling doctor, automobile, or home repair appointments, brief Internet searches, or sending directions to visiting relatives).

3.1.3.3. Educating or enhancing the professional skills of employees, (i.e., use of communication systems, work-related application training, etc.).

3.1.3.4. Sending messages on behalf of a chartered organization, (i.e., organizational Booster Club, Base Top 3, Base Company Grade Officers Association, etc.).

3.1.3.5. Limited use by deployed or TDY members for morale, health, and welfare purposes.

3.1.3.6. Job searching.

3.2. Inappropriate Use. Using the Internet for other than official or authorized use may result in adverse administrative or disciplinary action. The activities listed in paragraphs 3.2.1. through 3.2.13. involving the use of government-provided computer hardware or software are specifically prohibited. **Failure to observe the prohibitions and mandatory provisions of paragraphs 3.2.1 through 3.2.13 by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ),* Article 92, Failure to Obey Order or Regulation. Violations by ANG military personnel may subject members to prosecution under their respective State**

Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to local laws and the terms of the contract.

3.2.1. Use of Federal government communications systems for unauthorized personal use. See DOD 5500.7-R, *Joint Ethics Regulation (JER).*

3.2.2. Uses that would adversely reflect on the DOD or the Air Force such as chain letters, unofficial soliciting, or selling except on authorized Internet-based capabilities established for such use.

3.2.3. Unauthorized storing, processing, displaying, sending, or otherwise transmitting prohibited content. Prohibited content includes: pornography, sexually explicit or sexually oriented material, nudity, hate speech or ridicule of others on the bases of protected class (e.g., race, creed, religion, color, age, sex, disability, national origin), gambling, illegal weapons, militancy/extremist activities, terrorist activities, use for personal gain, and any other content or activities that are illegal or inappropriate.

3.2.4. Storing or processing classified information on any system not approved for classified processing.

3.2.5. Using copyrighted material in violation of the rights of the owner of the copyrights. Consult with the servicing Staff Judge Advocate for "fair use" advice.

3.2.6. Unauthorized use of the account or identity of another person or organization.

3.2.7. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.

3.2.8. Attempting to circumvent or defeat security or modifying security systems without prior authorization or permission (such as for legitimate system testing or security research).

3.2.9. Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

3.2.10. Permitting an unauthorized individual access to a government-owned or government-operated system.

3.2.11. Modifying or altering the network operating system or system configuration without first obtaining written permission from the administrator of that system.

3.2.12. Copying and posting of FOUO, CUI, Critical Information (CI), and/or PII on DOD–owned, –operated, or –controlled publically accessible sites or on commercial Internet-based capabilities.

3.2.13. Downloading and installing freeware/shareware or any other software product without DAA approval.

3.3. Official Use, Authorized Use, and Use of Internet-Based Capabilities. Official use of Internet-based capabilities unrelated to public affairs is permitted. However, because these interactions take place in a public venue, personnel acting in their official capacity shall maintain

liaison with their public affairs and operations security staff to ensure organizational awareness. Use of Internet-based capabilities for official purposes shall:

3.3.1. Comply with guidance in AFI 10-701, *Operations Security*, AFI 33-322, *Records Management*, AFI 33-364, *Records Disposition-Procedures and Responsibilities*, AFI 33-332, *Privacy Act Program*, and AFMAN 33-363, *Management of Records*.

3.3.2. Be consistent with the requirements of DOD 5500.7-R, *Joint Ethics Regulation (JER*).

3.3.3. Comply with public affairs Internet-based capabilities guidance.

3.3.4. Ensure that the information posted is relevant and accurate and provide no information not approved for public release, including personally identifiable information (PII).

3.3.5. Provide links to official Air Force content hosted Air Force-owned, -operated, or –controlled sites where applicable.

3.3.6. Include a disclaimer when personal opinions are expressed (e.g., "This statement is my own and does not constitute an endorsement by or opinion of the Air Force or the Department of Defense").

3.3.7. Air Force personnel may subscribe to official government-sponsored news, mail lists, and discussion groups. Some of these products are managed and approved by SAF/PA and accessible from the Air Force Link (**http://www.af.mil**). Using non-government subscription services without prior approval is misuse of a government system. Subscription or participation in subscription services will be in support of official duties only.

3.4. Managing Web Content. Information systems provide the capability to quickly and efficiently disseminate information. Web content must be managed in compliance with all information management policies and procedures including AFMAN 37-104, *Managing Information to Support the Air Force Mission*.

3.4.1. All DOD telecommunications systems and information systems are subject to monitoring for authorized purposes as prescribed by AFI 33-200, *Information Assurance (IA) Management* and AFI 10-712, *Telecommunications Monitoring and Assessment Program (TMAP)*. Prominently display the exact notice and consent banner specified in AFI 10-712, *Telecommunications Monitoring and Assessment Program (TMAP)* on the first page of all private/intranet web homepages. Notice and consent requirements do not apply to publicly accessible web sites/pages.

3.4.2. The publication of web content available to the public must comply with AFI 35-107, *Public Web Communications* and AFI 35-102, *Security and Policy Review Process* in addition to the official use policies in this chapter.

Chapter 4

VOICE COMMUNICATIONS SERVICES

4.1. Calls From Base Telephones.

4.1.1. Do not discuss classified or critical information over an unsecured telephone.

4.1.2. Long Distance Calls From Base Telephones.

4.1.2.1. Use the Defense Switched Network (DSN), not commercial long distance carriers, to call other DOD activities unless DSN service is not available in a timely manner. Use the DSN system only for official business or when in the best interest of the government.

4.1.2.2. User will contact their Telephone Control Officer (TCO) to obtain a personal identification number (PIN) for accessing commercial long distance voice service. This service is authorized for official uses only.

4.1.2.3. Callers without direct long distance dialing capability must request a control or billing account number from their TCO. Give the control or billing account number to the base switchboard operator when making a call.

4.1.2.4. For verification purposes, document all commercial long distance calls on AF Form 1072, *Authorized Long Distance Telephone Calls*. This is only required when PINs are not established or the host base does not have the capability to capture source caller identification information for each call.

4.2. Collect Calls to Base Telephones. The installation commander provides local guidance for official collect calls.

4.3. Personal Calls Over Official Telephones.

4.3.1. All government communications systems are subject to monitoring, interception, search, and seizure for all authorized purposes, reference Directive-Type Memorandum 08-060, *Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement*. Commanders and supervisors may allow personal calls during work hours using official telephones if:

4.3.1.1. The telephone call does not interfere with official duties.

4.3.1.2. The calls do not exceed reasonable duration and frequency, and whenever possible, are made during the employee's personal time such as after-duty hours or lunch periods.

4.3.1.3. The telephone calls serve a legitimate public interest (such as usage reduces time away from the work area or improves unit morale).

4.3.1.4. The telephone call does not reflect adversely on DOD or the Air Force (e.g., uses involving pornography; unofficial advertising, soliciting, or selling; and discussion of classified information).

4.3.1.5. The government does not incur any long distance or per-call charges above and beyond normal local charges. Normal local charges are based upon historical averages.

4.3.1.6. Personal calls may be made for "morale purposes" during deployments and TDYs as authorized by the organizational commander, see paragraph 4.9. for specific guidance.

4.4. Cordless Telephones Guidance.

4.4.1. The installation CSO, or designated representative, approves the use of cordless telephones on a case-by-case basis. For security purposes, the use of cordless phones on military installation work centers is highly discouraged. Cordless telephones can be "stepped-on" due to limited frequency allocation and overlapping of voice frequencies. Cordless telephones used outside the United States and Possessions will be host nation approved.

4.4.2. Use of cordless phones for command and control (C2) is prohibited.

4.4.3. Operating cordless phones within a classified environment will be certified for use by the installation Emission Security (EMSEC) manager within the Wing IA office.

4.5. Commercial Cellular Telephone (CT) Service.

4.5.1. **Organizations must request host base CSO approval before purchasing commercial cellular equipment.**

4.5.2. Personal calls to CT service providers from the host base official service may be authorized if the Air Force does not incur a long-distance toll or per-call charge. Cellular telephone services that provide per-call charges by billing the originating (calling) party, should be limited by the host base voice information system to official calls only.

4.5.3. Official Use of CT Service.

4.5.3.1. Use CT services only when it is the most cost-effective way to provide necessary communications or mobility is required.

4.5.3.2. Do not use an unclassified CT for C2 purposes. For security purposes, use a regular telephone (land line) as a first priority when and where available.

4.5.3.3. Do not transmit classified or critical information over unsecured CTs.

4.5.3.4. Minimize use of government-issued CTs while operating a moving vehicle. Comply with local policies, on or off-base.

4.5.4. Personal Use of CT Service.

4.5.4.1. The same rules that govern use of land line telephones apply to the use of Air Force CTs. Reference paragraph 4.9. for official and authorized purposes.

4.5.4.2. Members making inappropriate CT calls, text messages, or emails are subject to disciplinary action even if the usage does not cause additional expense. **Failure to observe the prohibitions and mandatory provisions of paragraph 4.5.4.2.1 by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ)*, Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to local laws and the terms of the contract.**

4.5.4.2.1. Do not use Air Force issued CTs to conduct personal commercial activities. Some examples of inappropriate calls include those related to personal solicitation or sales matters and those of a harassing or obscene nature. If a caller has any questions concerning proper use of government cell phones, it is the caller's responsibility to check with a supervisor before making the call.

4.5.4.3. Dual line CTs. Individuals may elect at their option to activate the secondary line as a personal number and place personal calls on that line.

4.5.4.3.1. Activation of a dual-number capability is not permitted on secure CTs.

4.5.4.3.2. Authorized end user of a government-owned, dual-number capable CT:

4.5.4.3.2.1. Shall sign an agreement, produced in accordance with Base Judge Advocate and Contracting office guidance, that contains appropriate "hold harmless" and "personal liability" clauses, prior to being issued a dual-number capable CT, without regard to whether or not the user elects to immediately activate the secondary number capability.

4.5.4.3.2.2. Must ensure all bills associated with the personal account are mailed directly to the user's home address or post office box if a secondary number is activated.

4.5.4.3.2.3. Shall ensure that the personal account is closed and the secondary number zeroized by the vendor prior to returning the CT to the local Personal Wireless Communications System (PWCS) manager for reuse when a CT is no longer required for the performance of duties.

4.6. Official Telephone Service in Personal Quarters is permitted for certain officials when necessary for national defense purposes. Contact your organizational TCO for more information. Specific policy and procedures are contained in AFI 33-111, *Voice Systems Management*.

4.7. Unofficial Commercial Telephone/Voice Service In Quarters.

4.7.1. The individual subscriber must pay for renting, acquiring, and maintaining end-user instruments, as well as all usage charges for personal telephone service.

4.7.2. If required by the housing manager, housing occupants must restore telephone wiring and outlets to the original configuration before clearing quarters.

4.8. Air Force Instruction on Defense Switched Network (DSN) On- or Off-Net Calling.

4.8.1. Authorized Actions:

4.8.1.1. Placing an official call to a DSN operator (base operator) from a commercial network and having the operator extend the call over DSN to a DSN number (on-netting).

4.8.1.2. Placing an official call to a DSN operator from a DSN number and having the operator extend the call to a local commercial number (off-netting).

4.8.1.2.1. The installation CSO determines local guidance on the off-netting of an official DSN call to an official long-distance toll number. The installation CSO is directly responsible for toll charges and determines billing procedures, recourse for

reimbursement, and/or acceptable appropriated fund support for off-netting official installation toll calls.

4.9. Health, Morale, and Welfare (HMW) Calls.

4.9.1. HMW calls are authorized over the DSN as prescribed in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C, *Policy for Department of Defense Voice Networks with Real Time Services (RTS)*. HMW calls are not authorized on government-issued CT, or via the FTS-2001 (or its designated replacement) network. However, satellite phones may be approved for HMW calls by the Organizational Commander on a case-by-case basis. You can obtain copies of CJCS publications at **http://www.dtic.mil/doctrine/index.html**.

4.9.1.1. HMW calls are intended for military and Department of the Air Force civilians. HMW calls are authorized when:

4.9.1.1.1. In an unaccompanied status at overseas or remote geographic locations.

4.9.1.1.2. Single at overseas or remote geographic locations.

4.9.1.1.3. Performing temporary duty (TDY).

4.9.1.2. Immediate family members or the parents of single active duty personnel and/or the guardian of the child of a single parent or military/military couple, both of whom are deployed, may be permitted to participate in the HMW program under procedures established by the Airman and Family Readiness Center (i.e., as part of "Hearts Apart" or similar programs) and the host commander. It is both the deployed commander and the host base commander's responsibility to provide guidance on the limitations and opportunities made available by this program.

4.9.1.3. The primary method for placing HMW calls is Automated Health and Morale System (AHAMS). AHAMS eliminates the need for base operator involvement and automatically controls time limits. If AHAMS is not available then place DSN HMW calls at routine precedence, normally not to exceed 15 minutes.

4.9.1.4. DSN HMW calls should not exceed a reasonable frequency as designated by the installation commander in conjunction with the installation CSO. Reasonable frequency is based upon installation/theater policy and determined by system capabilities, mission needs and restrictions. ***EXCEPTION:*** Emergency calls may exceed the established threshold.

4.9.1.5. Extending DSN HMW calls to a commercial number (off-netting) is authorized, provided it does not interfere with operational requirements. Off-net DSN HMW calls will not incur a toll charge to the government even if the intent is to reimburse the government. If the call incurs a toll charge, base operators may extend the call if the caller uses a credit/calling card to charge the call or the called party agrees to accept the charges (e.g., reversing of charges). See paragraph 4.8.1.2 for definition of off-netting.

4.9.1.6. On-netting of DSN HMW calls is permissible when placed from within the Continental United States (CONUS) as part of Airman and Family Readiness "Hearts Apart" or other similar programs. See paragraph 4.8.1.1. for definition of on-netting.

4.10. Official Government Issued Calling Card Use.

4.10.1. Government issued calling cards are issued for official use only. Cardholders must not use the calling card for any purpose other than official use. **Failure to observe the prohibitions and mandatory provisions of this paragraph by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ),* Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws**. **Violations by contactor personnel will be handled according to local laws and the terms of the contract.**

4.10.2. Cardholders must sign a statement acknowledging receiving the government issued calling card and that the card is for official use only.

Chapter 5

RECORDS MANAGEMENT

5.1. Records Management. Records management will be established as applicable for Air Force External Official Presence and for Air Force-wide, -operated, or –controlled publically accessible Internet sites. All uses must comply with AFI 33-322, AFI 33-332, AFI 33-364, and AFMAN 33-363. Records play a vital role in managing and operating Air Force activities. In simple terms, records document official business, serve as the memory of the organization, a record of past events, and are the basis for future actions. Every Air Force activity must manage its records to comply with legal accountability requirements. The key to an effective records management program is the integrity of the filing system--a system that ensures a standard methodology for filing, storing, discovering, retrieving, and ultimately disposing of records according to published retention and disposition schedules. Discovery of records must be facilitated by the creator of the information asset by assuring that metadata describing the information is captured or generated. AFMAN 33-363 establishes the requirement to use the Air Force Records Information Management System (AFRIMS); establishes guidelines for managing all records (regardless of media); and defines methods and the format for record storage, file procedures, converting paper records to other media or vice versa, and outlines the minimum to comply with records management legal and policy requirements.

5.1.1. All personnel:

5.1.1.1. Will receive annual government records management and PII training.

5.1.1.2. Must not conceal, remove, mutilate, obliterate or destroy government records without proper authority. Unauthorized concealment, removal, mutilation, obliteration or destruction of records, or any attempt to do so, may be a violation of Title 18, U.S.C., Section 2071 and may be punished by up to three years confinement and a fine. **Violations by military personnel are a violation of the *Uniform Code of Military Justice (UCMJ)*, Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel will be handled according to local laws and the terms of the contract.**

5.1.1.3. Must inform officials of any actual or potential unlawful removal, change, or destruction of Air Force records.

5.1.1.4. Must distinguish government records from non-record materials and maintain personal papers separately. Contact your Records Custodian for assistance.

5.1.1.5. Be aware of the periodic expiration of certificates if encryption is used or if encrypted electronic messages are received. Expiration is currently every 3 years or earlier based on expiration of individual employment. Recommend users store electronic messages in the unencrypted form or plan to de-encrypt encrypted electronic messages prior to expiration of encryption certificate. Otherwise, when the encryption certificate is needed the user has to go through the key recovery process (through the appropriate ESD or CST Help Desk) to gain the necessary keys to access encrypted electronic messages.

5.2. Records Authentication. The process used to ascertain the identity of a person or the integrity of specific record information. A record is authenticated when it contains an official signature or seal indicating the document is genuine and official. A signature or seal may be written, stamped, electronic or digital. Reference AFI 33-321.

Chapter 6

ELECTRONIC MESSAGING

6.1. General. All government communications systems are subject to monitoring, interception, search, and seizure for all authorized purposes, reference DOD Chief Information Officer (CIO) Memorandum, *Policy on Use of Department of Defense (DOD) Information Systems Standard Consent Banner and User Agreement*. Government-provided messaging systems are for official use and limited authorized personal use only. (See Chapter 3.)

6.1.1. AFMAN 33-363 defines official records and electronic records. DOD 5400.7-R_AFMAN 33-302, *Freedom of Information Act Program*; and AFI 33-332, *Air Force Privacy Program*, describe when electronic messages are subject to the requirements of the *Freedom of Information Act (FOIA)* and the *Privacy Act of 1974*.

6.1.2. Barring absence of official communication channels, do not use personal accounts to conduct official AF communication. Conduct personal communication in compliance with DOD 5500.7-R, *Joint Ethics Regulation (JER)*.

6.1.2.1. Avoid the dissemination and discussion of non-public information and disclaim opinions as necessary in accordance with DOD 5500.7-R.

6.1.2.2. Exercise vigilance to ensure that both sensitive and classified information are not inadvertently disclosed, and that the disclosure of unclassified information, in aggregate, does not reveal sensitive or classified information.

6.2. Air Force Messaging.

6.2.1. Electronic messaging (including email and instant messaging) users will:

6.2.1.1. Maintain responsibility for the content of their electronic messages and ensure that messages sent adhere to acceptable use of Internet-based capabilities (Chapter 3).

6.2.1.2. Maintain sent and received information according to Air Force records management directives: AFMAN 33-363; AFI 33-322, *Records Management Program*; and AFRIMS RDS (**https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**). Emails may be subject to requests under the FOIA, litigation, and court orders. If requested, individuals are responsible for reviewing messages in email accounts and all backups to locate responsive material.

6.2.1.3. Adhere to local policy on sending electronic messages to a large number of recipients. Digital images, as well as mass distribution of smaller messages, may delay other traffic, overload the system, and subsequently cause system failure.

6.2.1.4. Adhere to local policy when sending an electronic message to mail distribution lists. Use web pages or electronic public folders for unofficial electronic messages (i.e., booster club activities, etc.).

6.2.1.5. Only reply to electronic messages that absolutely require a response and minimize the use of the "Reply to All" function.

6.2.1.6. Bear sole responsibility for material sent.

6.2.1.7. Properly coordinate and staff electronic messages according to local directives.

6.2.1.8. Take appropriate action on non-delivery notices or message rejects to ensure messages reach the intended recipient.

6.2.1.9. Not auto-forward electronic messages from the ".mil" domain to a commercial Internet Service Provider (ISP).

6.2.1.10. Not indiscriminately release electronic messaging addresses to the public. For further information, reference the Air Force Freedom of Information Act "Release of Email Addresses" (**http://ww.foia.af.mil**).

6.2.2. Individual electronic messages are considered official when the sender is conducting mission-related or official business.

6.2.3. Special delivery instructions should be included as part of the message text to identify the specific addressee to whom the message is to be delivered.

6.2.4. Messages with special delivery instructions should not be distributed through normal delivery channels unless specifically requested by the recipient.

6.2.5. Special Handling Requirements. Do not transmit controlled unclassified information (i.e. Privacy Act, FOUO) on or to systems not approved for that information. Reference AFI 31-401.

6.2.5.1. Transmitting unclassified information on classified networks is authorized unless specifically prohibited by the network operating instructions. Follow AFI 31-401, *Information Security Program Management*, marking guidance for unclassified electronic messages sent across a classified network.

6.2.5.2. Identify all Privacy Act and For Official Use Only (FOUO) electronic messages in the subject line with FOUO.

6.3. Use of Subscription Services. Internet electronic messaging access grants users the ability to subscribe to a variety of news, mail lists, and discussion groups. These services may include professional groups sponsored by Air Force agencies and other newsgroups sponsored by non-Air Force agencies, including the DOD, other Federal agencies, educational institutions, and commercial activities (i.e., product information updates and technical newsletters).

6.3.1. When an extended absence will not allow access to your electronic messaging account, unsubscribe or suspend mail from any mail lists or newsgroups. This alleviates large backlogs of received messages that consume server storage resources.

6.3.2. Participation in newsgroups whose content is contrary to the standards set by DOD 5500.7-R (i.e., obscene, offensive, etc.) is prohibited. (See Chapter 3.) Organizational commanders may direct electronic messaging administrators to set up permanent blocks on a specific site or newsgroup addresses to prevent subscription to such services.

6.4. Electronic Message Format.

6.4.1. Electronic messages, to include official communications such as memorandums (letters), notes, messages, reports, etc., follow specific formats found in Air Force Handbook (AFH) 33-337, *The Tongue and Quill*, AFI 33-321, *Authentication of Air Force Records*, and AFMAN 33-326, *Preparing Official Communications.*

6.4.2. Senders should include a signature block on all official electronic messaging sent from individual or organizational accounts. Examples of appropriate signature blocks are in AFH 33-337, *The Tongue and Quill*.

6.4.2.1. Include "//SIGNED//" in upper case before the signature block to signify official Air Force information (e.g., instructions, directions, or policies).

6.4.2.2. Restrict the signature block to name, rank, service affiliation, duty title, organization name, phone numbers (DSN and/or commercial as appropriate), and social media contact information.

6.4.2.3. Do not add slogans, quotes, or other personalization to an official signature block.

6.4.3. When a member (military, civilian, or contractor) has another official position (i.e., civilian is a Reservist/Guardsman; contractor is a Reservist/Guardsman or vice versa), the member will be provided two email accounts in order to separate the member's email for each function. Signature blocks will explicitly follow the guidance in paragraph 6.4.2. to distinguish between the different official positions performed by a single member. Exception: Air Reserve Technicians may use their military accounts.

6.4.4. Naming conventions for messaging systems are covered in TO 00-33D-2001-WA-1, *Active Directory Naming Conventions*.

6.5. Protection and Disposition of Electronic Message Information.

6.5.1. Controlled Unclassified Messages. There is information, other than classified information, that has been determined to require some type of protection or control.

6.5.1.1. Encrypt electronic messages whenever practical when they contain controlled unclassified information, (i.e. Privacy Act, FOUO). See Chapter 2 for further information on encryption. See AFI 31-401 for additional guidance on controlled unclassified information.

6.5.1.2. Protecting FOUO Information. When transmitting FOUO information, add "FOUO" to the beginning of the subject line, followed by the subject. FOUO attachments shall be marked with a statement similar to this one: "FOR OFFICIAL USE ONLY ATTACHMENT." Additional protection methods may include password protecting the information in a separate portable document format supporting password protection. See AFI 31-401 for additional guidance on protecting FOUO information.

6.5.1.3. Protecting Personal Information. Transmitting personal information exempt from public release under the Freedom of Information Act must be marked "FOUO" at the beginning of the subject line IAW guidance contained in AFI 33-332, AFI 31-401 and DOD Manual 5200.01, V1, *DoD Information Security Program: Overview, Classification, and Declassification.*

6.5.1.3.1. Apply the following statement at the beginning of the message: "The information herein is For Official Use Only (FOUO) which must be protected under the Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or civil penalties."

6.5.1.3.2. Do not indiscriminately apply this statement to messages that are not publically releasable. Use it only in situations when you are actually transmitting personal information. Personal information may not be disclosed to anyone outside DOD unless specifically authorized by *The Privacy Act*.

6.5.1.3.3. Do not send Privacy Act information to distribution lists or group email addresses unless each member has an official need to know for the personal information.

6.5.1.4. Protecting Exempt *Freedom of Information Act (FOIA*) Information, Title 5, U.S.C., Section 552. Do not send FOIA information normally exempt in electronic messages without an appropriate level of protection to prevent unintentional or unauthorized disclosure. Refer to AFI 31-401 and DOD Manual 5200.01, V1 for additional guidance or consult your local FOIA representative. Appropriate level of protection includes proper marking and encryption.

6.5.2. Classified Electronic Messages.

6.5.2.1. Marking Classified Electronic Messages. Mark all classified electronic messages with a level of classification equivalent to the information they contain or reveal in accordance with AFI 31-401, DOD Manual 5200.01, V1, and Controlled Access Program Coordination Office (CAPCO) Register and Manual.

6.5.2.2. Message Declassification. Classified messages must contain declassification or downgrading instructions at the end of the message text. See AFI 31-401 for additional guidance.

6.5.2.3. Classified Electronic Message Destruction.

6.5.2.3.1. Destroy classified messages when no longer required. If the classified message is an official record, destroy it only after the retention period in AFRIMS RDS has expired.

6.5.2.3.2. TOP SECRET Control Officers use AF Form 143, *TOP SECRET Register Page*, or another approved form (e.g., AF Form 310, *Document Receipt and Destruction Certificate*) to record the destruction of TOP SECRET electronic messages.

6.5.2.3.3. When you must keep a record of destroyed SECRET and CONFIDENTIAL materials, use AF Form 310 or AF Form 1565, *Entry, Receipt and Destruction Certificate*.

6.5.3. Message Destruction.

6.5.3.1. Protect messages from unauthorized or unintentional disclosure or destruction.

6.5.3.2. Users must destroy messages according to AFRIMS RDS instructions located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. Contact your records custodian and/or IAO for proper destruction procedures. Message destruction at the system administration level may be implemented on behalf of the users according to AFRIMS RDS instructions.

6.6. Digitally Signing and Encrypting Electronic Messages.

6.6.1. Digitally Signing. Use PKI (Public Key Infrastructure) CAC digital signature certificates whenever it is necessary for the recipient of an electronic message to be assured of the sender's identity (non-repudiation) or have confidence the message has not been modified. Messages containing only unofficial information and not containing an embedded hyperlink and/or attachment are not required to be digitally signed. Refer to guidance in AFI 33-321 regarding email authentication. Contact your IAO for assistance. Examples of messages that should be digitally signed include:

6.6.1.1. Formal direction to a government employee or contractor.

6.6.1.2. Messages that stipulate an Air Force official position on any matter.

6.6.1.3. Messages that commit to, authorize, or deny the use of funds in some manner.

6.6.1.4. Emails from user accounts and systems which contain an embedded hyperlink and/or attachment. Plain-text references to URL's do not require digital signature but they are recommended.

6.6.2. Encrypting. DOD PKI-based encryption is not authorized for protecting classified information on systems not approved for that use. Encryption increases bandwidth and resource requirements; therefore, email encryption should be used to protect the following types of information, and the number of email recipients should be kept to a minimum:

6.6.2.1. For Official Use Only (FOUO).

6.6.2.2. Privacy Act Information. For additional guidance see AFI 33-332.

6.6.2.3. Personally Identifiable Information (PII), (see Terms, Attachment 1).

6.6.2.4. Individually identifiable health, DOD payroll, finance, logistics, personnel management, proprietary, and foreign government information.

6.6.2.5. Contract data.

6.6.2.6. Export controlled technical data or information.

6.6.2.7. Operations Security (OPSEC) information. Encrypt critical information, OPSEC indicators, and other sources of information. For additional guidance on OPSEC requirements see AFI 10-701, *Operations Security*.

6.6.2.8. Information specified for encryption by domain owners pertaining to your individual areas of responsibility, see AFPD 33-4, *Enterprise Architecting*.

6.7. Message Forwarding (Manual and Automated). All previously stated guidance also applies to forwarded electronic messages. If the message was originally encrypted, it should not be forwarded outside the organization without being encrypted again whenever practical. See paragraph 5.4.2.1. for further information on marking classified electronic messages.

6.7.1. Automated Message Forwarding.

6.7.1.1. Be aware that each message is automatically unsigned/unencrypted and distributed based on profiles loaded in the automated message distribution or profiling system.

6.7.1.2. Do not auto-forward official electronic messages to commercial Internet Service Providers (ISPs) from government computer systems.

6.7.1.3. Do not create automated message forwarding rules or procedures to send electronic messages to pagers, cell phones, commercial/non-military accounts.

6.8. Message Management. Electronic messages that are considered Air Force records IAW AFMAN 33-363 must be managed, stored, and deleted from the message system after copying to a record keeping system. If a digitally signed and/or encrypted official record is to be preserved, the user must follow procedures outlined in AFI 33-322, *Records Management Program*. These procedures will ensure the information necessary to validate the digital signature is retained and the record is always accessible.

6.8.1. Use backup media of messages for security, system restoration and short-term archiving of official record email not to exceed 120 days.

6.8.2. Users are required to retain official record emails by filing in an approved electronic record keeping system. If an approved electronic record keeping system is not available, users will print the official record emails to paper copy and file.

6.8.2.1. Management of both official and individual messages is determined by the Chief of an Office of Record and is based upon the message originator's authentication authority.

6.8.2.2. In determining whether a message is a record or not, focus on the content of the information and not on the method used to send it. If the content of the message would have been filed if it had been created on paper, then the message should also be filed or archived. Encrypted messages will be decrypted prior to electronically filing or archiving. In some cases an individual message may become background information to the final decision or recommendation. In other cases the message may be managed in a suspense document until all comments are received and incorporated into a final document, then filed under the appropriate table and rule in Air Force RDS.

6.8.2.3. Preserve the content, context, and structure of records in a useable format for their authorized retention period. A complete electronic messaging record will include the message itself, attachments (e.g., word processing and other electronic documents transmitted with the message), and transmission data (e.g., originator, recipients, addresses, date, and time).

6.8.2.4. Make records easily accessible by individuals who have an official need to access them.

6.8.2.5. Arrange electronic message records according to the approved file plan.

6.8.2.6. Ensure federal records sent or received on electronic messaging systems outside organizational control are preserved. Ensure reasonable steps are taken to capture available transmission and receipt data needed by the agency for record-keeping purposes.

6.9. Organizational Messaging. Organization SMTP mailboxes may be used for all organizational messaging requirements unless usage of DMS is required in support of combatant command responsibilities of CJCSI 5721.01E, *The Defense Message System and Associated Legacy Message Processing Systems*.

6.9.1. Each office will designate an individual to monitor the organization mailboxes regularly to ensure messages requiring action are promptly acted upon, to include electronic

filing and/or destruction, as defined in the organizational file plan and associated table and rule.

6.9.2. Each individual should have a unique identifier that the system can authenticate and provide an audit trail. When email systems cannot provide a unique identifier for actions with the organization mailboxes, local administrative procedures will provide the audit trail.

6.9.3. To assist with providing an audit trail for email users, personnel who send on behalf of the owner of an organizational account will send a copy of all email as "Cc" to the organizational mailbox.

WILLIAM T. LORD, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 5 United States Code, *Section 552a (Privacy Act)*, update January 7, 2011

Title 5, U.S.C., Section 552, *The Freedom of Information Act*

Title 44, U.S.C. § 3301, *Definition of Records*

CNSSI 4009, *National Information Assurance (IA) Glossary*, April 26, 2010

DOD Manual 5200.01, V1, *DoD Information Security Program: Overview, Classification, and Declassification*, February 24, 2012

DOD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1, 1993

DODI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003

DODI 8520.2, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, April 1, 2004

DOD 5400.7-R_AFMAN 33-302, *Freedom of Information Act Program*, October 21, 2010

Directive-Type Memorandum 08-060, *Policy on Use of Department of Defense (DOD) Information Systems Standard Consent Banner and User Agreement*, 9 May 2008, **http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-060.pdf**

CJCSI 5721.01E, *The Defense Message System and Associated Legacy Message Processing Systems*

CJCSI 6215.01C, *Policy for Department of Defense Voice Networks with Real Time Services (RTS)*, November 9, 2007

AFJI 31-102, *Physical Security*, May 31, 1991

AFPD 33-1, *Information Resources Management*, June 27 ,2006

AFPD 33-2, *Information Assurance (IA) Program*, August 3, 2011

AFPD 33-4, *Enterprise Architecting*, June 27, 2006

AFI 10-701, *Operations Security*, June 8, 2011

AFI 10-712, *Telecommunications Monitoring and Assessment Program (TMAP)*, June 8, 2011

AFI 31-401, *Information Security Program Management*, November 1, 2005

AFI 33-106, *Managing High Frequency Radios, Personal Wireless Communication Systems, And The Military Affiliate Radio System*, January 9, 2002

AFI 33-111, *Voice Systems Management*, 2 March 24, 2005

AFI 33-112, *Information Technology Hardware Asset Management*, January 7, 2011

AFI 33-200, *Information Assurance (IA) Management*, December 23, 2008

AFI 33-321, *Authentication of Air Force Records*, August 3, 2011

AFI 33-322, *Records Management Program*, October 7, 2003

AFI 33-332, *Air Force Privacy Act Program,* May 16, 2011

AFI 33-364, *Records Disposition-Procedures and Responsibilities,* December 22, 2006

AFI 35-102, *Security and Policy Review Process,* October 20, 2009

AFI 35-107, *Public Web Communications,* October 21, 2009

AFI 36-3026_IP, Volume 1, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*, June 17, 2009

AFI 51-303, *Intellectual Property--Patents, Patent Related Matters, Trademarks and Copyrights*, September 1, 1998

AFH 33-337, *The Tongue and Quill*, August 1, 2004

AFMAN 33-282, *Computer Security (COMPUSEC)*, March 27, 2012

AFMAN 33-326, *Preparing Official Communications*, November 25, 2011

AFMAN 33-363, *Management of Records*, March 1, 2008

AFMAN 37-104, *Managing Information to Support the Air Force Mission,* June 1, 1995

Prescribed Forms

AF Form 4394, *Air Force User Agreement Statement – Notice and Consent Provision*, July 31, 2009

Adopted Forms

AF Form 847, *Recommendation for Change of Publications;* AF Form 1565, *Entry, Receipt and Destruction Certificate;* AF Form 143, *TOP SECRET Register Page*, 19820901 V1 – 11 March 2003; AF Form 310, *Entry, Receipt and Destruction Certificate*, 19951101 V4 – 1 November 1995; AF Form 1072, *Authorized Long Distance Telephone Calls*, 19730801 V4 – 1 August 1973; AF Form 4433, *US Air Force Unclassified Wireless Mobile Device User Agreement*; DD Form 2875, *System Authorization Access Request (SAAR)*

Abbreviations and Acronyms

AFH—Air Force Handbook

AFPD—Air Force Policy Directive

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFRIMS—Air Force Records Information Management System

ANG—Air National Guard

C2—Command and Control

CAC—Common Access Card

CBT—Computer-Based Training

CFP—Communications Focal Point

CI—Critical Information

CIO—Chief Information Officer

CIPS—Cyberspace Infrastructure Planning System

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

COMPUSEC—Computer Security

CONUS—Continental United States

CSO—Communications and Information Systems Officer

CT—Cellular Telephone

CUI—Controlled Unclassified Information

DAA—Designated Accrediting Authority

DISA—Defense Information Systems Agency

DMS—Defense Message System

DOD—Department of Defense

DODI—Department of Defense Instruction

DSN—Defense Switched Network

EMAIL—Electronic Mail

EMSEC—Emission Security

FIPS—Federal Information Processing Standard

FOIA—Freedom of Information Act

FOUO—For Official Use Only

GFE—Government Furnished Equipment

GIG—Global Information Grid

HIPAA—Health Insurance Portability and Accountability Act (HIPAA),

HMW—Health, Morale, and Welfare

IA—Information Assurance

IAO—Information Assurance Officer

IP—Information Protection

IS—Information System

IT—Information Technology

MAJCOM—Major Command

NIPRNET—Non-secure Internet Protocol Router Network

OPSEC—Operation Security

PA—Privacy Act

PED—Portable Electronic Device

PII—Personal Identifiable Information

PII—Personally Identifiable Information

PIN—Personal Identification Number

PKI—Public Key Infrastructure

PWCS—Personal Wireless Communications System

RDS—Records Disposition Schedule

SAF—Secretary of the Air Force

SCI—Sensitive Compartmented Information

SIPRNET—Secret Internet Protocol Router Network

SMTP—Simple Mail Transport Protocol

TCO—Telephone Control Officer

TDY—Temporary Duty

UCMJ—Uniform Code of Military Justice

US—United States

U.S.C.—United States Code

USAF—United States Air Force

USM—Unit Security Manager

USB—Universal Serial Bus

Terms

Accountable Officer—An individual appointed by proper authority who maintains item records and/or financial records in connection with Government property, irrespective of whether the property is in his or her possession for use or storage, or is in the possession of others to whom it has been officially entrusted for use or for care and safekeeping. (AFI 33-112)

Authorized User—Any appropriately cleared individual with a requirement to access a DOD information system in order to perform or assist in a lawful and authorized governmental function. (DODD 8500.01)

Air Force—Global Information Grid (AF-GIG)— The Air Force-provisioned portion of the Global Information Grid (GIG) that the Air Force has primary responsibility for the procurement, operations, and defense. It provides global connectivity and services, in addition to C2 of that connectivity and those-services that enable Air Force commanders to achieve information and decision superiority in support of Air Force mission objectives. The AF-GIG consists of fixed, mobile, and deployable facilities, and equipment, as well as processes, trained personnel and information.

Client Support Technician (CST)—CSTs support customers with resolving issues relating to information technology devices, such as personal computers, personal digital assistants, and printers.

Clearance—Formal certification of authorization to have access to classified information other than that protected in a special access program (including SCI). Clearances are of three types: confidential, secret, and top secret. A top secret clearance permits access to top secret, secret, and confidential material; a secret clearance, to secret and confidential material; and a confidential clearance, to confidential material. (CNSSI 4009)

Collaborative Computing—Applications and technology (e.g., whiteboarding, group conferencing) that allow two or more individuals to share information real time in an inter- or intra-enterprise environment. (CNSSI 4009)

Common Access Card (CAC)—A Department-wide smart card used as the identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DOD civilian employees, eligible contractor personnel, and eligible foreign nationals; the primary platform for the public key infrastructure authentication token used to access DOD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment; and the principal card enabling physical access to buildings, facilities, installations, and controlled spaces. (DODI 8520.2)

Communications and Information Systems Officer (CSO)—The designated official who has overall responsibility for communications and information support at any given level of the Air Force (base, tenant, MAJCOM, USAF, etc.). At base level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities. At MAJCOM and other activities responsible for large quantities of communications and information systems, it is the person designated by the commander as responsible for overall management of communications and information systems budgeted and funded by the MAJCOM or activity. CSOs are the accountable officer for all automated data processing equipment in their inventory and are responsible for maintenance of the communications blueprint through the use of the Cyberspace Infrastructure Planning System (CIPS).

Controlled Unclassified Information (CUI)— Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. (DOD Manual 5200.01, Vol 1)

Designated Accrediting Authority (DAA)—Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. Synonymous with Designated Approving Authority and Delegated Accrediting Authority. (AFPD 33-2)

Domain—A functional area of responsibility. (AFPD 33-4)

Emission Security (EMSEC)—The protection resulting from all measures taken to deny

unauthorized personnel information of value that might be derived from communications systems and cryptographic equipment intercepts and the interception and analysis of

compromising emanations from cryptographic—equipment, information systems, and

telecommunications systems. (AFI 33—200)

Emission Security (EMSEC) Manager—The designated person responsible for the management of EMSEC; usually part of Wing IA Office.

Encryption—The process of changing plaintext into ciphertext for the purpose of security or privacy. (CNSSI 4009)

Enterprise Service Desk (ESD)—The AF Tier 1 helpdesk providing computer support for AFNet users experiencing computer, email, or network problems.

GIG—The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network. (CNSSI 4009)

Information—1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

Information Assurance (IA)—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (CNSSI 4009 and DODD 8500.01)

Information Assurance Officer (IAO)—An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DOD information system or organization. While the term IAO is favored within the DOD, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer). (DODI 8500.2)

Information System (IS)—Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections. (DODD 8500.01)

Information Technology (IT)—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (CNSSI 4009)

Internet-based Capabilities (IbC)— All publicly-accessible information capabilities or applications available across the Internet in locations not owned, operated, or controlled by DoD or the Federal government. IbC includes collaborative tools such as social networking services,

social media, user generated content, social software, e-mail, instant messaging, and discussion forums (e.g., Facebook, MySpace, Twitter, Google Applications).

Mobile Computing Device—IS devices such as personal electronic devices, laptops, and other handheld devices that can access AF managed networks through mobile access capabilities and can store data locally.

Modification—A temporary or permanent change to a system that is still being produced. The purpose of the modification is to correct deficiencies, improve reliability and maintainability, or to improve capabilities. (AFI 33-150)

Non-Record Materials—U.S. Government-owned documentary materials excluded from the legal definition of records or not meeting the requirements of that definition. Include extra copies of documents kept only for convenience of reference, stocks of publications and of processed documents, and library or museum materials intended solely for reference or exhibition; also called non-record copies or non-records. (See Title 44 United States Code [U.S.C.] 3301, *Definition of Records.*)

Personal Identifiable Information (PII)—Any information about an individual maintained

by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an

individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. For DOD information assurance purposes, electronic PII records are categorized according to the potential negative impact of loss or unauthorized disclosure according to FIPS Pub 199. (AFI 33—200)

Personal Wireless Communications System (PWCS)—A user centric service that is accessible via devices either vehicular mobile, hand carried, or worn by individual users. Each user may have an individually identifiable electronic address. (AFI 33-106)

Portable Electronic Device (PED)—Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDAs, cellular/Personal Communications Service phones, two-way pagers, electronic mail (email) devices, audio/video recording devices, and hand-held/laptop computers. (DODD 8100.02)

Protected Workplace—Workplaces that minimally satisfy Physical and Environmental

Controls for Confidentiality Level Sensitive as established in DODI 8500.2., AFJI 31—102, and

AFI 31—401 provide additional guidance for physical and information security, respectively. (AFI 33-200)

Public Key Infrastructure (PKI)—The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. (CNSSI 4009)

Records—All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the US Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. May also be called Federal records that exclude Presidential records and records of the U.S. Congress. (AFI 33-322)

Records Custodian—The individual responsible for physical custody, maintenance, and disposition of records accumulated in the performance of a particular function. The directorate/separate office/activity records officer designates the files custodian in designating the directorate "office of record." Depending upon the size and complexity of the directorate, the RM may elect to designate more than one office of record/files custodian for the records it holds. (AFI 33-322)

Removable Media—Portable electronic storage media such as magnetic, optical, and solid state devices, which can be inserted into and removed from a computing device for the purpose of storing text, video, audio, and image information. Such devices lack independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar USB storage devices. (CNSSI 4009)

Sensitive Information— Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under *Title 5 U.S.C.* Section 552a (Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy. **Note:** Systems that are not national security systems, but contain sensitive information are subject to be protected in accordance with the requirements of the Computer Security Act of 1987 (Public Law 100-235). See also controlled unclassified information. (CNSSI 4009)

Telephone Control Officer (TCO)—Individual who authorizes and controls long distance telephone toll calls within a unit.

User—All users who use or have access to a government Information System and government computer devices, to include government desktop and laptop computers, mobile devices and email systems.